(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 993 142 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
12.04.2000 Bulletin 2000/15

(51) Int. Cl.[7]: **H04L 9/00**

(21) Application number: **99307101.8**

(22) Date of filing: **07.09.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **14.09.1998 US 153272**

(71) Applicant:
LUCENT TECHNOLOGIES INC.
Murray Hill, New Jersey 07974-0636 (US)

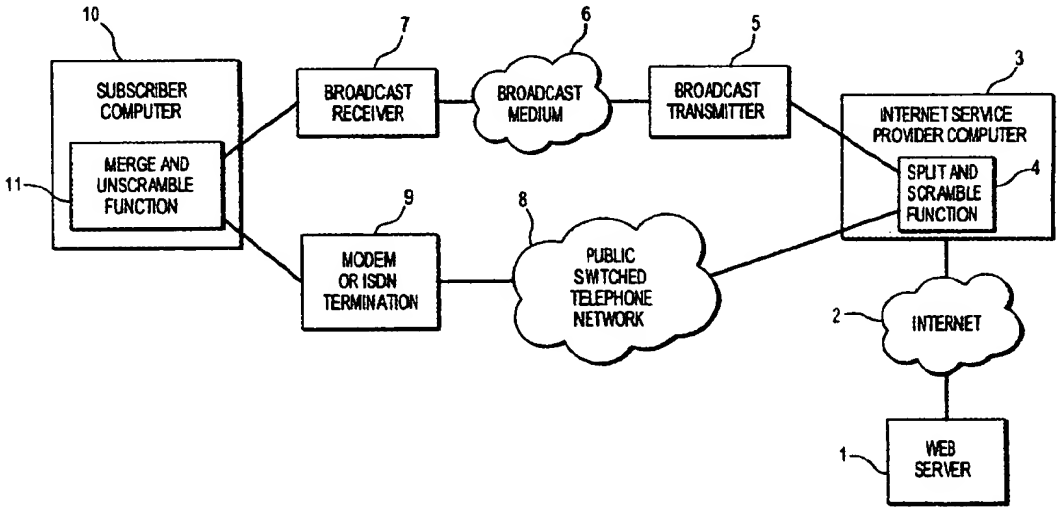
(72) Inventor:
Witschorik, Charles Arthur
Naperville, Illinois 60563 (US)

(74) Representative:
Watts, Christopher Malcolm Kelway, Dr. et al
Lucent Technologies (UK) Ltd,
5 Mornington Road
Woodford Green Essex, IG8 0TU (GB)

(54) Safe transmission of broadband data messages

(57) An arrangement for providing secure transmission of information. The bulk of the information is transmitted over non-secure channels such as broadcast media which terminate on a plurality of receiving stations. However, a residue of data is transmitted over a protected channel, such as a point-to-point channel, established for example, by a telephone connection. Interception of a complete message, when only the bulk of the message is available, becomes very difficult. It becomes even more difficult if scrambling arrangements are used to select the particular bits of the data message that are transmitted over the secure channel. It becomes still more difficult, if the data transmitted over the secure channel, itself, alters the scrambling algorithm.

FIG. 1



EP 0 993 142 A1

Description

Technical Field:

[0001] This invention relates to methods and apparatus for transmitting data messages in such a way that interception is virtually impossible.

Problem:

[0002] With the increased use of the Internet, and especially of the Internet as used to transmit broadband data signals, the necessity for avoiding unauthorized interception of such messages becomes ever more critical. Methods have been proposed using a decryption key which is reliably transported to a destination. A message that has been encrypted using a corresponding encryption key, and sent over an interceptible medium, then requires that the message be decrypted by an authorized recipient, who has the key, or an unauthorized recipient, who does not have the key. Various encryption schemes have been proposed, but the ever increasing power of modem computers makes unauthorized decryption an ever increasing threat. Much of the information from the Internet will be broadcast into a plurality of homes over a shared medium such as a co-axial cable, an optical fiber cable, or wireless, having the characteristic that it is easy for unauthorized recipients to intercept the raw signal that is not destined for them. A problem of the prior art, therefore, is that it is difficult to prevent unencrypted signals which are broadcast to a plurality of destinations from being illegally intercepted by an unwanted destination; even intercepted encrypted messages may no longer be safe from decryption by unwanted users.

Solution:

[0003] The above problem is solved, and an advance is made over the prior art in accordance with this invention wherein a fraction of the data that is to be transmitted from a source to a destination is withheld from a broadcast medium, and is instead transmitted over a more secure and private medium such as a telephone connection; the data received over the broadcast medium is then combined with the data that had been withheld from the broadcast medium, but transmitted over the secure medium in order to derive the complete data message. Advantageously, such an arrangement makes decryption essentially imposs-ible since the interceptor cannot access the full data of the data message. In many cases, the secure connection exists as an upstream connection for controlling the source of the data message; by using this upstream connection as a two-way connection, a separate downstream connection is conveniently formed to convey the data that had been withheld from the broadcast medium.

[0004] In accordance with one embodiment of the invention, the full data is first scrambled before a regular and repetitive portion of the data is extracted to be withheld from the broadcast medium, and to be transmitted over the secure medium. Advantageously, such an arrangement makes partial decryption much more difficult.

Brief Description of the Drawing:

[0005]

Figure 1 is a block diagram, illustrating the principles of Applicant's invention.

Detailed Description:

[0006] Figure 1 is a block diagram illustrating the operation of the invention. A source of the data message 1, such as a Web Server, transmits a data message over the Internet to an Internet Service Provider (ISPN) Computer 3. The Computer includes software, or hardware for performing a split and scramble function 4, and the split signal is then sent partly to the broadcast transmitter 5, and partly over the point-to-point public switched telephone network 8. The bulk of the data goes to the broadcast transmitter 5, which transmits this data over a broadcast medium 6 (such as a co-axial cable, a fiber optic cable, a radio channel, and a combination of ones of these media). From the broadcast medium, a broadcast receiver 7 receives the broadcast portion of the data signal. The public switched telephone network 8 transmits the non-broadcast portion to a modem, or an integrated services digital network (ISDN) termination 9. The output of the broadcast receiver 7 and the modem, or ISDN termination, is transmitted to a subscriber computer 10 which includes a merge and unscramble function 11, to combine the two signals in order to reconstitute the original data signal.

[0007] The connection from the subscriber computer to the ISP computer, and thence to the source of the data, is made in the course of establishing the connection between the subscriber computer and the source. The source being identified by a URL (Universal Resource Locator) number. This makes the use of this arrangement very practical since no extraneous connections are required.

[0008] In order to make the scheme even more foolproof, the data that is transmitted over the secure channel can be used to specify the splitting arrangement. For example, suppose that every 19th bit is transmitted over the secure channel; initially the first bit that is received over the secure channel could be inserted into the 10th bit position of the 19 bits received from both the secure and non-secure channel. Then, if that bit is zero, a subsequent bit received over the secure channel, could be inserted in the 11th bit of the next group of 19 bits transmitted over the secure and non-secure channel. If the

bit received over the secure channel were a 1, then the next bit received over the secure channel would be inserted in the 9th position of the next group of 19 bits transmitted over the secure and non-secure channel. Thus, the secure information actually specifies the splitting arrange-ment between the secure and the non-secure information, greatly increasing the difficulty of successfully intercepting and decrypting the transmitted information. The splitting and merging operations are, of course, synchronized.

[0009] Alternatively, or additionally, the segments of the total message can be scrambled. With simple scrambling, the order of bits is changed in each segment before transmitting; the unscrambling process then reorders the received bits of each segment to be in the original order, with the bit received over the secure channel being inserted in a fixed position of each segment.

[0010] Alternatively, scrambling itself may be influenced by the content of the secure channel. For example, if the secure channel signal is a 1, then a first scrambling algorithm is used on the data of a corresponding, or succeeding segment over the non-secure channel; if it is 0, a second scrambling algorithm. Multiple scrambling algorithms based on several bits of the secure channel can also be used.

[0011] Scrambling and splitting according to the contents of the secure channel can be combined. For example, the splitting arrangement described above can precede a scrambling operation prior to transmitting a scrambled segment over the non-secure channel. The contents of the non-secure channel are then unscrambled at the receiver and the bit received over the secure channel is inserted into its appropriate position in accordance with the insertion scheme described above.

[0012] On top of the technique for splitting in accordance with data transmitted over the secure channel and/or the scrambling technique, both described above, the whole message can be encrypted, thus, further complicating the task of the interceptor. Even without encryption, if the secure channel remains secure, and the splitting period is not the same as the period of sub-sections of the data, (e.g., one byte long), the encryption of a message based on the broadcast channel information only, should continue to be very difficult.

[0013] Many variations of the preferred embodiment will be apparent to those of ordinary skill in the art. The invention is limited only by the attached Claims.

Claims

1. Apparatus for transmitting data comprising:

   a non-secure connection for transmitting the bulk of the data;
   a secure connection for transmitting the residue of the data;
   means for splitting a data signal into a first signal representing the bulk of the data, and a second signal representing the residue of the data;
   means for combining the first signal, and the second signal into a combined signal representing all of the data;
   wherein said means for splitting the data transmits the bulk of the data over said non-secure connection, and transmits the residue of the data over said secure connection.

2. The apparatus of Claim 1, wherein:

   the first signal is transmitted over a broadcast connection receivable by a plurality of receivers; and
   the second signal is transmitted over a point-to-point connection receivable by only a single receiver.

3. The apparatus of Claim 1, wherein said means for splitting, comprises means for generating a scrambled second signal.

4. The apparatus of Claim 3, wherein said means for generating a scrambled signal comprises means for generating a scrambled signal dependent on the contents of the data transmitted by the second signal.

5. The apparatus of Claim 1, wherein the means for splitting the data signal performs a split that is dependent on the contents of the data transmitted by the second signal.

6. A method for reliably transmitting and receiving data comprising the steps of:

   splitting a data signal representing said data into a first signal representing the bulk of the data, and a second signal representing the residue of the data;
   transmitting the first signal over an unprotected medium;
   transmitting the second signal over a protected medium;
   receiving the first and second signals; and
   combining the first signal and the second signal into a combined signal representing said data.

7. The method of Claim 6, wherein the step of transmitting the first signal comprises the step of:

   transmitting the first signal over a broadcast medium, receivable by a plurality of receivers; and
   wherein the step of transmitting the second signal comprises the step of transmitting the sec-

ond signal over a connection receivable by only a single receiver.

8. The method of Claim 6, wherein said step of splitting said data signal comprises the step of scrambling data of said first signal.

9. The method of Claim 8, wherein said signal step of scrambling data of said first signal, comprises scrambling as determined by the contents of the data transmitted by the second signal.

10. The method of Claim 6, wherein said step of splitting said data signal comprises the step of splitting the data signal dependent on the contents of the data transmitted by the second signal.

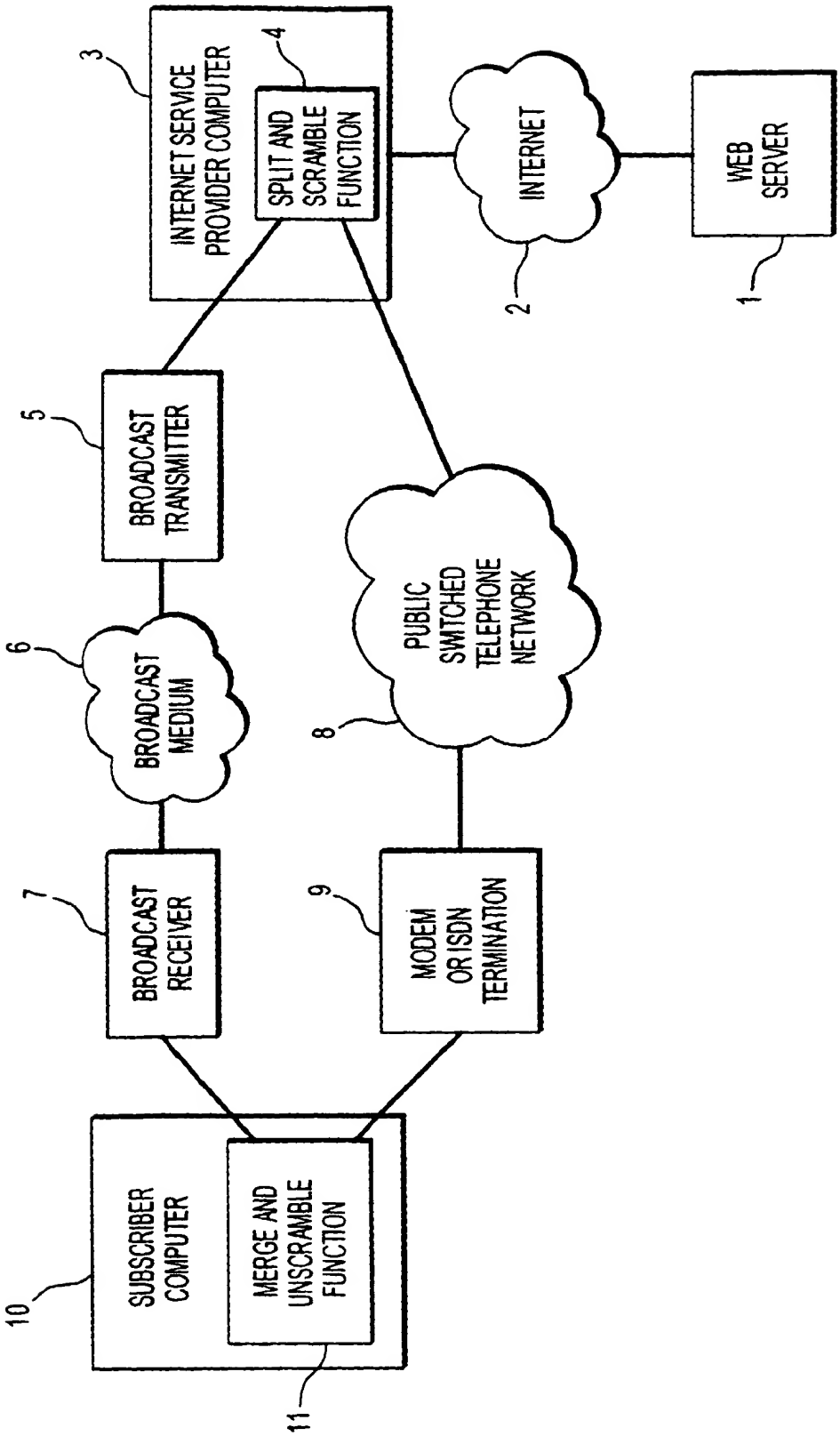


FIG. 1

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 30 7101

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	GB 2 222 057 A (CARRIDICE LTD) 21 February 1990 (1990-02-21) * the whole document *	1,2,6-8	H04L9/00
X	WO 98 25372 A (VOLTAIRE ADVANCED DATA SECURIT) 11 June 1998 (1998-06-11) * abstract * * page 10, line 4 - line 24 * * page 14, line 7 - line 11 * * page 14, line 17 - line 25 * * page 15, line 9 - line 13 *	1,2,6,7	
A	"DATA COMMUNICATIONS LINE SHUFFLER" IBM TECHNICAL DISCLOSURE BULLETIN,US,IBM CORP. NEW YORK, vol. 33, no. 3A, August 1990 (1990-08), page 443-444 XP000120546 ISSN: 0018-8689 * the whole document *	1,3,6,8	
A	YAMAMOTO H: "ON SECRET SHARING COMMUNICATION SYSTEMS WITH TWO OR THREE CHANNELS" IEEE TRANSACTIONS ON INFORMATION THEORY,US,IEEE INC. NEW YORK, vol. IT-32, no. 3, May 1986 (1986-05), page 387-393 XP000764636 ISSN: 0018-9448 * page 387, left-hand column, line 17 - right-hand column, line 6 *	1,6,9	TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04L H04K

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	21 December 1999	Holper, G

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 99 30 7101

This annex lists the patent family members relating to the patent documents cited in the above–mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

21-12-1999

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2222057 A	21-02-1990	NONE	
WO 9825372 A	11-06-1998	US 5969632 A	19-10-1999
		AU 5065998 A	29-06-1998
		EP 0948771 A	13-10-1999

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82